

SHIsFileAvailableOffline

Vulnerable to TOCTOU issues

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-04-17

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 6282 bytes

Attack Category	<ul style="list-style-type: none">Path spoofing or confusion problem		
Vulnerability Category	<ul style="list-style-type: none">Indeterminate File/PathTOCTOU - Time of Check, Time of Use		
Software Context	<ul style="list-style-type: none">File Management		
Location			
Description	<p>SHIsFileAvailableOffline() determines whether a file or folder is available for offline use. It also determines whether the file would be opened from the network, from the local Offline Files cache, or from both locations.</p> <p>SHIsFileAvailableOfflin() is vulnerable to TOCTOU attacks.</p>		
APIs	Function Name	Comments	
	SHIsFileAvailableOffline	check	
Method of Attack	<p>The key issue with respect to TOCTOU vulnerabilities is that programs make assumptions about atomicity of actions. It is assumed that checking the state or identity of a targeted resource followed by an action on that resource is all one action. In reality, there is a period of time between the check and the use that allows either an attacker to intentionally or another interleaved process or thread to unintentionally change the state of the targeted resource and yield unexpected and undesired results.</p>		
Exception Criteria			
Solutions	Solution Applicability	Solution Description	Solution Efficacy
	Generally applicable.	Utilize a file descriptor versions of file operations	Effective.

1. <http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html> (Barnum, Sean)

		whenever possible.	
	Generally applicable.	The most basic advice for TOCTOU vulnerabilities is to not perform a check before the use. This does not resolve the underlying issue of the execution of a function on a resource whose state and identity cannot be assured, but it does help to limit the false sense of security given by the check.	Does not resolve the underlying vulnerability but limits the false sense of security given by the check.
	Generally applicable.	Limit the interleaving of operations on files from multiple processes.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.
	Generally applicable.	Limit the spread of time (cycles) between the check and use of a resource.	Does not eliminate the underlying vulnerability but can help make it more difficult to exploit.
	Generally applicable.	Recheck the resource after the use call to verify that the action was taken appropriately.	Effective in some cases.
Signature Details		HRESULT SHIsFileAvailableOffline(LPCWSTR pszPath, LPDWORD pdwStatus);	

Examples of Incorrect Code	<pre>LPCWSTR pszPath = L"\\\\alpha.com\\beta\\gamma"; [...] DWORD status; HRESULT result = SHIsFileAvailableOffline(pszPath, &status); [...] FILE *theFile = _wopen(pszPath, L"r");</pre>	
Examples of Corrected Code	<pre>LPCWSTR pszPath = L"\\\\alpha.com\\beta\\gamma"; [...] FILE *theFile = _wopen(pszPath, L"r");</pre>	
Source Reference	<ul style="list-style-type: none"> http://msdn.microsoft.com/library/default.asp?url=/library/en-us/shellcc/platform/shell/reference/functions/shisfileavailableoffline.asp² 	
Recommended Resource	<ul style="list-style-type: none"> MSDN reference for SHIsFileAvailableOffline³ 	
Discriminant Set	Operating System	<ul style="list-style-type: none"> Windows
	Languages	<ul style="list-style-type: none"> C C++

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>